DENNIS K. BURKE
United States Attorney
District of Arizona

FREDERICK A. BATTISTA
Maryland State Bar Member
PETER S. SEXTON
Arizona State Bar No. 011089
JAMES R. KNAPP
Arizona State Bar No. 021166
Assistant U.S. Attorneys
Two Renaissance Square
40 North First Avenue, Suite 1200
Phoenix, Arizona 85004
Telephone: (602) 514-7500
Fred.Battista@usdoj.gov
Peter.Sexton@usdoj.gov
James.Knapp2@usdoj.gov

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

United States of America, Plaintiff, v. Daniel David Rigmaiden, et al., Defendants.	No. CR-08-0814-PHX-DGC **GOVERNMENT'S MEMORANDUM REGARDING LAW ENFORCEMENT PRIVILEGE AND REQUEST FOR AN *EX PARTE* AND *IN CAMERA* HEARING IF NECESSARY**

The United States, through undersigned counsel, submits this memorandum in support of its request for an *ex parte* and *in camera* hearing, if necessary, and to answer the Court's questions set forth at the February 10, 2011, status conference. In particular, the Court requested guidance with respect to two primary issues: (1) the propriety of holding an *ex parte* and *in camera* hearing to address the United States' assertion of a law enforcement privilege with respect to the operation of the equipment used to locate the Verizon Wireless broadband access card ultimately found in defendant Daniel David Rigmaiden's apartment; and (2) the factors the Court should consider in balancing the asserted privilege with any possible Fourth Amendment rights of defendant Rigmaiden.

To provide the necessary context, this memorandum also describes, in some detail, how law enforcement officers tracked the Verizon Wireless broadband access card (hereinafter "the aircard") to defendant's apartment in Santa Clara, California, and explains why defendant's request for additional discovery is unwarranted. Should the Court desire to review additional

information, the United States is simultaneously filing, under seal, the original search warrant materials for defendant's California residence and the two Court Orders obtained in the Northern District of California, which authorized the use of the equipment used to locate the aircard.

Respectfully submitted this 11th day of March, 2011.

DENNIS K. BURKE
United States Attorney
District of Arizona

S/Frederick A. Battista

FREDERICK A. BATTISTA
PETER S. SEXTON
JAMES R. KNAPP
Assistant U.S. Attorneys

MEMORANDUM

I. Facts.

Until his arrest on August 3, 2008, and later identification via fingerprint analysis and a criminal records check, the actual identity of defendant Rigmaiden was unknown to his fellow co-conspirators and the federal agents who pursued him. As a result, defendant was referred to by all as "the Hacker." Prior to his arrest, defendant was the leader of an incredibly sophisticated electronic federal tax return fraud scheme. In the course of the scheme, defendant submitted well over 1,200 fraudulent tax returns to the Internal Revenue Service ("IRS") using stolen identities (including the identities of persons both living and deceased), used his computer expertise to e-file the fraudulent returns through unsuspecting host computers and thereby hide the location of his initial point of access to the internet, and further sought to hide his involvement through the use of bank accounts and bank cards acquired through various co-conspirators.

A. Identifying the Aircard.

In June 2007, an IRS e-file provider notified the IRS of a large volume of tax returns filed through its website using what appeared to be an automated process. Multiple fraudulent returns were filed from single IP addresses within short time periods. This procedure indicated the use of a computerized bulk filing system. The IP addresses were traced to locations all across the United States, suggesting that most of the IP addresses were not the true source of the fraudulent returns. For tax year 2007, the IRS identified 1,272 returns, 175 IP addresses, and 73 bank accounts believed to be linked to the scheme.

One of the fraudulent returns from June 2007 was filed from IP address 75.208.204.165. This IP address drew the attention of the investigators because it appeared to have been used in isolation, whereas other IP addresses apparently used in support of the scheme were used multiple times within a short time period. IRS agents subpoenaed the subscriber information and learned that the IP address was associated with a Verizon Wireless broadband access card provided to a "Travis Rupard" in San Jose, California.

As IRS agents continued to investigate, the participants in the scheme continued to file more fraudulent returns. IRS agents subpoenaed the subscriber information for four additional fraudulent returns filed in March 2008, and the IP addresses were traced back to the same Travis Rupard aircard. "Travis Rupard" turned out to be a false identity: the subscriber information ultimately led to a non-existent address and a California driver's license number assigned to a female with a different name.

B. The Hacker's False Identities.

On April 15, 2008, agents executed a search warrant on a co-conspirator's computer and reviewed e-mail correspondence between the co-conspirator and the defendant, known then only as the Hacker. In the e-mails, defendant claimed that he had produced and sold fraudulent identification documents for many years, and that he knew "everything there is to know about creating new identities in the USA." Very soon thereafter, the co-conspirator agreed to cooperate against defendant and has thereafter been known throughout the investigation and this prosecution as CI-2.

On April 17, 2008, defendant contacted CI-2 via a secure e-mail account and provided detailed encrypted instructions for delivering $68,000 in proceeds from the scheme to defendant. Defendant directed CI-2 to: (1) wash the currency in lantern fuel to remove any drug or explosive residue that could draw the attention of law enforcement; (2) vacuum seal the currency and place it in the cavity of a gift-wrapped toy; and (3) attach a birthday card written to suggest that the package was a gift for a dying child. Shortly thereafter, on May 5, 2008, defendant further directed CI-2 to address the package to a "Patrick Stout" and send it by FedEx to arrive the next day at a particular FedEx/Kinko's store in Palo Alto, California. Upon further investigation, "Patrick Stout" was determined to be another false identity used by defendant. Specifically, the investigation team traced the identity to a post office box in Sacramento, California, opened by "Patrick Stout" through the use of a fraudulent California driver's license bearing a number assigned to a female with a different name.

The package containing $68,000 in currency was delivered to the FedEx/Kinko's store

on May 6, 2008. On May 7, 2008, at approximately 5:00 a.m., a then unknown white male, average build, wearing a dark jacket with a hood, who appeared to be in his twenties and soon presented identification in the name "Patrick Stout," was observed entering the back entrance of the Fed Ex/Kinko's on foot and retrieving the package. The male carried the box to a nearby corner where he ripped open the box, removed the contents containing the currency and discarded the packaging in a nearby dumpster. The then unknown male proceeded toward a nearby train station. Agents conducting surveillance were unsuccessful in efforts to identify the then unknown male or follow him to his final destination.

On or about May 8, 2008, defendant e-mailed CI-2 and confirmed receipt of the money. Defendant indicated in his e-mail the money was picked up by a third party/courier. In light of the fact that similar clothing worn by the "courier" was later found in defendant's apartment, along with some of the original $100 dollar bills that were part of the $68,000 shipment, and the Patrick Stout drivers license, the investigation team now believes that defendant personally picked up the $68,000.

As the investigation progressed, on or about June 25, 2008, agents obtained the Travis Rupard aircard transaction logs and compared them with transaction information for other activities tied to defendant, such as e-mail communications with CI-2, online bank account logins for one or more accounts related to the scheme, and additional e-filed fraudulent tax returns. The IP address connections and date/time stamps were consistent, showing that defendant was, indeed, using the Travis Rupard aircard.

C. Locating the Aircard.

1. The Relevant Technology.

Cellular telephone networks provide service to their customers through antennas deployed across the provider's coverage area. When the user places an outbound call, the handset transmits that communication over the airwaves to a nearby tower antenna, which relays the call to a local switch for routing. Conversely, whenever another party places a call to a user's cellular telephone, the network "pages" that phone to alert the owner to the incoming call; if the

owner answers, the call is put through and (as before) carried by a tower near the phone. In either scenario, a phone may move in the course of a single call through the coverage areas of multiple towers, especially where the user is in a moving vehicle. In most instances, the network enables seamless "handoffs" from one tower to the next without the user's knowledge. As a result, the system's awareness of a wireless phone's general whereabouts is essential to providing cellular service.

Spacing between antenna towers varies enormously depending on a number of factors, especially terrain and population density. In a heavily populated area such as lower Manhattan, towers may be spaced every few hundred yards; in rural areas, by contrast, towers may be separated by 20 miles or more; and towers in suburban or small urban areas will typically be spaced in a range between those extremes.

Except in sparsely populated areas, a typical tower will have three separate antenna faces (also called sectors), with each face serving a 120-degree portion of the roughly circular coverage area extending out from the antenna mast. For many carriers, the three sectors can be visualized as the areas on a clock face from 10 to 2; from 2 to 6; and from 6 to 10. In rural coverage areas, a tower may simply have a single 360-degree face.

Whenever a cellular phone user initiates or receives a communication – such as a voice call or text message – the carrier routinely creates a record, including the date and exact time, of the tower and sector handling the communication at the start and end of the communication. Service providers typically retain these routine business records for several months or longer. In addition to these historical records, carriers have certain legal obligations with respect to prospective – that is, real-time – location information sought by law enforcement. Specifically, the FCC requires carriers to be technically capable of delivering real-time cell-site data at the start and end of calls.

Whether obtained prospectively or from historical records, cell-site records cannot reveal a phone's exact location. As noted above, even in heavily populated urban centers a tower's service radius is several hundred yards. Moreover, because of variable factors such as terrain

and network congestion, the tower serving a particular communication is not necessarily the tower closest to the phone. [1/]

2. The Tracking Operation.

In July 2008, the United States obtained historical cell site information to find the aircard. On July 10, 2008, Magistrate Judge Lawrence O. Anderson issued an order pursuant to 18 U.S.C. § 2703(d) requiring Verizon Wireless to turn over historical cell site and sector/distance information for the aircard. On July 16, 2008, Magistrate Judge Edward C. Voss issued a similar order for additional historical records. Verizon provided the requested information in each instance to the FBI via e-mail.

Using this historical information, an FBI agent used generally known characteristics of cell tower ranges in order to prepare a cell tower range chart. The chart was based on historical cell tower data and simple estimates of the range of the three cell towers used most frequently by the subject aircard. Defendant has been provided a copy of the chart and the raw data used to create it.

The United States also sought real-time cell site information. On July 11, 2008, Magistrate Judge Richard Seeborg of the Northern District of California, San Jose Division, issued two orders (as noted above, filed separately this date under seal). The first authorized a tracking device warrant under Federal Rule of Criminal Procedure 41(b), finding probable cause to believe that the monitoring of the aircard would lead to evidence and the identification of the perpetrator of the subject scheme. The Order authorized the monitoring of transmissions related to the location of the aircard, including the monitoring of the aircard while the agents were stationed in public locations and the aircard was inside a private residence, garage, or other location not open to the public or visual surveillance. The second Order, issued under 18 U.S.C. §§ 2703(c), 2703(d), 3122, and 3123, authorized the installation of a pen register and trap and

---

[1/] Some service providers can provide more precise location information – referred to as GPS or E911 information – but the United States did not request or obtain any of that information in this case.

trace device for the aircard. This Order authorized the gathering of cell site information while incoming and outgoing calls were in progress, but did not authorize the investigative agency to obtain any cell site information that might be available while the aircard was turned "on" but a call was not in progress, information that would allow it to triangulate antenna tower locations, or Global Position System ("GPS") information regarding the location of the aircard.

FBI personnel completed tracking the aircard on July 16, 2008, using equipment known as a pen register and trap and trace device. The details of the actual equipment, its operation, its capabilities and the identities of the operators, are all law enforcement sensitive. The United States can confirm, however, that the operators never used more than a single piece of equipment at any one time, and therefore, employed no triangulation techniques through the use of multiple devices. In the course of the operation to locate the aircard, the personnel also did not obtain any GPS data from Verizon Wireless.

D. The Domicilio Apartment Complex in Santa Clara, California

Using the pen register and trap and trace device, FBI personnel tracked the aircard to the "Domicilio" apartment complex in Santa Clara, California. The personnel were observed by the members of investigation team. The investigation team members have all been disclosed to defendant but not the FBI personnel who actually operated the subject equipment. Using the law enforcement sensitive equipment, the FBI personnel were able to determine that the subject aircard was operating within an area the size of three to four apartments within the Domicilio Apartment Complex. The FBI personnel did not operate the subject equipment in a manner that would allow them to precisely determine the location within a particular apartment. The FBI personnel only advised the investigation team of the area noted immediately above.

Soon after the FBI personnel completed their work on July 16, 2008, members of the investigation team obtained rental and utility information for three of the subject apartments. The agents also subpoenaed the rental agreements and related files for the three apartments, which included copies of the occupants' driver's licenses and 2006 tax returns.

The applicant for Apartment No. 1122 fit the profile for the Hacker. Among many

factors, the applicant/occupant,"Steven Travis Brawner," appeared to be a white male in his twenties, and on his rental application he claimed to be a software engineer. Second, in support of this rental application, the occupant had provided the landlord with a fake California driver's license bearing a number traced back to a female with a different name. Third, handwriting on the apartment rental application was similar to the handwriting on a "Patrick Stout" post office box application. Fourth, the Social Security number provided by the applicant was assigned to a Steven Brawner who died in 1997. Finally, the occupant had provided a 2006 tax return for "Steven Travis Brawner" but IRS records showed that the return had never been filed.

E. Discovery Provided.

The United States has already exceeded its discovery obligations under the applicable federal rules, statutes, and case law. It has disclosed all preservation requests, subpoenas, applications, court orders, warrant returns, and raw data obtained during the tracking operation.

II. Law and Argument.

A. The Information Sought By Defendant Is Protected By Law Enforcement Privilege.

Defendant argues that, in addition to the discovery already produced, he needs detailed information about the United States' electronic surveillance techniques used in this case, including specifications and capabilities of the devices used, the names and contact information for all individuals involved in the surveillance, and an explanation of exactly how law enforcement used the devices and analyzed the relevant data to find the subject aircard.

The Supreme Court, in United States v. Roviaro, recognized an "informer's privilege" that protects the identity of government informants:

> What is usually referred to as the informer's privilege to withhold from disclosure the identity of persons who furnish information of violations of law to officers charges with enforcement of that law. The purpose of the privilege is the furtherance and protection of the public interest in effective law enforcement.

Roviaro, 353 U.S. 53, 59 (1957). If "disclosure of an informer's identity, or the contents of his communication, is relevant and helpful to the defense of an accused," however, the privilege does not apply. *Id.* at 60-61.

Courts have since extended the qualified privilege in Roviaro to cover other investigative techniques, including traditional and electronic surveillance. For example, in United States v. Green, the D.C. Circuit upheld the privilege over the defendant's request to learn the location of an observation post used in a drug investigation:

> Just as the disclosure of an informer's identity may destroy his future usefulness in criminal investigations, the identification of a hidden observation post will likely destroy the future value of that location for police surveillance. The revelation of a surveillance location might also threaten the safety of police officers using the observation post, or lead to adversity for cooperative owners or occupants of the building. Finally, the assurance of nondisclosure of a surveillance location may be necessary to encourage property owners or occupants to allow the police to make such use of their property.

670 F.2d 1148, 1155 (D.C. Cir. 1981). In United States v. Van Horn, the Eleventh Circuit recognized that the privilege applies to electronic surveillance as well and upheld the privilege over the defendant's request to learn the type and placement of microphones in a co-defendant's office. *See* 789 F.2d 1492, 1507 (11th Cir. 1986) ("Disclosing the precise locations where surveillance devices are hidden or their precise specifications will educate criminals regarding how to protect themselves against police surveillance.").

B. An *Ex Parte* and *In Camera* Hearing To Resolve The Privilege Claim Is Appropriate.

An *in camera* hearing is an appropriate method to resolve the United States' claim of law enforcement privilege. *See, e.g.,* Van Horn, 789 F.2d at 1508 (district court held *in camera* hearing); In re Department of Homeland Security, 459 F.3d 565, 569-71 (5th Cir. 2006) (instructing the district court in a civil case to "review the documents at issue *in camera* to evaluate whether the law enforcement privilege applies"); *cf.* United States v. Klimavicius-Viloria, 144 F.3d 1249, 1261 (9th Cir. 1998) ("*Ex parte* hearings are generally disfavored. In a case involving classified documents, however, *ex parte, in camera* hearings in which government counsel participates to the exclusion of defense counsel are part of the process that the district court may use in order to decide the relevancy of the information.") (citation omitted); In re Grand Jury Subpoenas Dated March 19, 2002 and August 2, 2002, 318 F.3d 379, 386 (2nd Cir. 2003) (describing the presentation of documents for *in camera* review as a "practice

both long-standing and routine in cases involving claims of privilege" and citing illustrative cases).

To assess both the applicability of the subject privilege and the need for the materials, the court should review the materials in question or hold an evidentiary hearing in chambers. Frequently, because filing documents under seal may inadequately protect particularly sensitive information, the court may, in the exercise of its informed discretion and on the basis of the circumstances presented, require that the party possessing the materials appear *ex parte* in chambers to submit the materials for *in camera* review by the judge. In re The City of New York, 607 F.3d 923, 948-49 (2d Cir 2010) (an appropriately general docket entry memorializing any *ex parte* proceedings can be entered in the public records of the district court so long as it does not compromise the interests of the party holding the confidential information, or the public. *Id.* at 949 n.25). At the *ex parte in camera* hearing, the United States will be available to present more detailed information about the operation of the subject equipment and related materials through management personnel, and its concerns about disclosure.

C. In Determining Whether The Law Enforcement Privilege Applies, The Court Must Balance a Defendant's Need For The Information With The Public Interest In Keeping The Information Private.

As noted above, the privilege is qualified. The public interest in keeping the information private must be balanced against a defendant's articulated need for the information. *See* Roviaro, 353 U.S. at 628-29. "Whether a proper balance renders nondisclosure erroneous must depend on the particular circumstances of each case, taking into consideration the crime charged, the possible defenses, the possible significance of the [privileged information], and other relevant factors." *Id.* at 629. The court will essentially consider the defendant's "need [for] the evidence to conduct his defense and [whether] there are . . . adequate alternative means of getting at the same point. The degree of the handicap [to the defendant] must then be weighed by the trial judge against the policies underlying the privilege." United States v. Harley, 682 F.2d 1018, 1020 (D.C. Cir. 1982); *see also* United States v. Cintolo, 818 F.2d 980, 1002 (1st Cir. 1987) (the question is "whether the [defendant] demonstrate[s] an authentic 'necessity,' given

the circumstances, to overbear the qualified privilege"); United States v. Foster, 986 F.2d 541, 543 (D.C. Cir. 1993) (balancing defendant's need for information against importance of government's interest in avoiding disclosure).

In the civil context, courts have employed a ten-factor balancing test to resolve claims of law enforcement privilege. *See, e.g.,* In re U.S. Department of Homeland Security, 459 F.3d 565, 570-71 (5th Cir. 2006) (referring to the 10-part standard as the "Frankenhauser test," after Frankenhauser v. Rizzo, 59 F.R.D. 339, 344 (E.D. Pa. 1973)). The test examines the following factors:

> (1) the extent to which disclosure will thwart governmental processes by discouraging citizens from giving the government information; (2) the impact upon persons who have given information of having their identities disclosed; (3) the degree to which governmental self-evaluation and consequent program improvement will be chilled by disclosure; (4) whether the information sought is factual data or evaluative summary; (5) whether the party seeking discovery is an actual or potential defendant in any criminal proceeding either pending or reasonably likely to follow from the incident in question; (6) whether the police investigation has been completed; (7) whether any intradepartmental disciplinary proceedings have arisen or may arise from the investigation; (8) whether the plaintiff's suit is non-frivolous and brought in good faith; (9) whether the information sought is available through other discovery or from other sources; and (10) the importance of the information sought to the plaintiff's case.

Id.; see also Tuite v. Henry, 98 F.3d 1411, 1417 (D.C. Cir. 1996) (ordering district court to use the Frankenhauser test). Some courts have held that once the government has established the applicability of the law enforcement privilege, the public's interest in minimizing disclosure creates a "pretty strong presumption against lifting the privilege," a presumption that may be rebutted only if the party seeking discovery shows a compelling need. *See* In re The City of New York, 607 F.3d 923, 945 (2nd Cir. 2010) (citing the final three Frankenhauser factors as dispositive of the party's showing of need); Dellwood Farms, Inc. v. Cargill, Inc., 128 F.3d 1122, 1125 (7th Cir. 1997); *cf.* Black v. Sheraton Corp. of America, 564 F.2d 531, 545 (D.C. Cir. 1977) (beginning analysis "with the proposition that there is indeed a public interest in minimizing disclosure of documents that would tend to reveal law enforcement investigative techniques or sources").

Even if the party seeking disclosure successfully rebuts the presumption (by a showing

of, among other things, a "compelling need"), the court must still then weigh the public interest in non-disclosure against the need of the litigant for access to the privileged information before ultimately deciding whether disclosure is required. In re The City of New York, 607 F.3d at 948.

D. In This Case, The Public Interest in Nondisclosure Significantly Outweighs Defendant's Interest in the Information.

Here, the public interest in nondisclosure significantly outweighs defendant's need for the information. The FBI has always asserted that its electronic surveillance and cell-site tracking capabilities and equipment are law-enforcement sensitive. In addition, FBI policy dictates that the technically trained agents who operate the cell-site tracking devices are considered a covert resource and are not to be placed into chain of custody for evidence or other situations that will require testimony. The mere fact that some information related to the technology is publicly available does not mean that defendant is entitled to detailed information about who used the device in this case, and how it was used. Even where some aspects of a protected technique are known to the public, "[t]here is no principle . . . that requires an agency to release all details of a technique simply because some aspects are known to the public." Barnard v. Department of Homeland Security, 598 F.Supp.2d 1, 23 (D.D.C. 2009). *See also* Piper v. Department of Justice, 294 F.Supp.2d 16, 31 (D.D.C. 2003) (finding that FBI properly withheld information about sensitive electronic monitoring devices under FOIA despite general knowledge of devices because "[g]eneral, non-specific knowledge that the FBI possesses capabilities to electronically monitor the movement of automobiles, for example, or other moving objects is not the same as identifying the actual device, its function, and its capabilities").

In addition, disclosure of the information would diminish the future value of these investigative techniques, allow individuals to devise measures to counteract these techniques in order to evade detection, discourage cooperation from third parties and other governmental agencies who rely on these techniques in critical situations, and possibly lead to other harmful

consequences not suitable for inclusion in this response. The risk of circumvention of an investigative technique if information is released has been accepted by numerous courts as a basis for non-disclosure. *See, e.g.*, James v. U.S. Customs and Border Protection, 549 F.Supp.2d 1, 10 (D.D.C. 2008) (concluding that CBP properly withheld information under FOIA that "could enable [others] to employ measures to neutralize those techniques"); Judicial Watch v. U.S. Department of Commerce, 337 F.Supp.2d 146, 181-82 (D.D.C. 2004) (permitting Department of Commerce to withhold information because disclosure could risk future circumvention and explaining that "even commonly known procedures may be protected from disclosure if the disclosure could reduce or nullify their effectiveness").

Defendant also claims the information is Brady material because he might be able to use it in a pretrial motion to suppress, apparently hoping that he can identify some error in how the United States located the aircard. Even if defendant were to obtain the detailed information he seeks, however, it could not lead to suppression of any evidence in this case. First, the electronic surveillance techniques only led the investigative team to the general proximity of the subject aircard, obtained and maintained by defendant through the use of a false identity, while defendant was aware it would have to communicate with Verizon Wireless in order to function. Therefore, defendant had no expectation of privacy with respect to the general proximity of the aircard due to the fact that the device would have to be able to advise Verizon Wireless of its general location in order to communicate with the firm's cell towers, and function as designed and intended. Second, even if defendant had any expectation of privacy, the United States acted in good faith in relying on and executing a tracking device warrant founded on probable cause. Third, any attacks on the United States' actions or legal authority under statutory provisions including 18 U.S.C. § 2703 would not result in suppression of evidence.

1. Defendant does not need the privileged information because he has no reasonable expectation of privacy in the cell site location information.

Defendant had no reasonable expectation of privacy concerning the general proximity of the aircard for three reasons: (1) since the Supreme Court's holding in United States v. Knotts,

courts have repeatedly held that people do not have a reasonable expectation of privacy concerning their general location; (2) people do not have a reasonable expectation of privacy concerning information voluntarily turned over to third-party businesses, which includes the cell site data at issue in the present case; and (3) defendant has no reasonable expectation of privacy in the location of an aircard obtained and maintained under a fictitious identity.

a. Location.

"The application of the Fourth Amendment depends on whether the person invoking its protections can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action." Smith v. Maryland, 442 U.S. 735, 740 (1979). In United States v. Knotts, the Supreme Court held that warrantless use of a tracking device in a public space did not implicate the Fourth Amendment. *See* 460 U.S. 276, 281 (1983). In Knotts, law enforcement officers used a beeper to monitor the location of a can of chloroform (a precursor chemical used to manufacture illicit drugs) as it traveled in a car along public highways from one defendant's residence to another defendant's secluded cabin in Wisconsin. *See* 460 U.S. at 278. Once the beeper arrived at the cabin, the officers discontinued its use. *Id.* They surveilled the cabin for three days and then obtained a search warrant. *Id.* at 279. The Court recognized some privacy interest in the car and the cabin, but held that the warrantless monitoring of the beeper did not violate the Fourth Amendment because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* at 281; *see also* United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004) (citing Knotts and holding that cell-site data is simply a proxy for the defendant's visually observable location and defendant had no legitimate expectation of privacy in his movements along public highways while government agents simultaneously tracked his cell phone), *vacated on other grounds by* Garner v. United States, 543 U.S. 1100 (2005).

In United States v. Karo, the Court applied this analysis to a tracking device located within a private space. *See* 468 U.S. 705 (1984). In Karo, the government installed and monitored a beeper in a can of ether, which was picked up by the defendant and moved to his

house. *Id.* at 708. The can was later moved to other houses and then to a locker in a commercial storage facility, although the beeper was not sensitive enough to indicate in which particular locker the can was located. *Id.* The Court held that the defendant had a reasonable expectation of privacy in his private residence, so warrantless monitoring of the beeper inside his home violated his Fourth Amendment rights. *Id.* at 714. But the Court also held that the monitoring of the beeper inside the storage facility was permissible, even though the defendant had an expectation of privacy in his own storage locker:

> Monitoring the beeper revealed nothing about the contents of the locker that Horton and Harley had rented and hence was not a search of that locker. FN6 The locker was identified only when agents traversing the public parts of the facility found that the smell of ether was coming from a specific locker.
>
> FN6. Had the monitoring disclosed the presence of the container within a particular locker the result would be otherwise, for surely Horton and Harley had a reasonable expectation of privacy in their own storage locker.

Id. at 720-21 & n.6. Thus, tracking a beeper does not implicate the Fourth Amendment merely because it happens to be located in a private space; rather, a tracking of a beeper implicates the Fourth Amendment when it reveals information about that private space or discloses its particular location within it.

Here, defendant had no reasonable expectation of privacy in the general proximity of the aircard within the Domicilio apartment complex. As in Knotts and Karo, the cell site information did not disclose any information about defendant's apartment, or even disclose the exact location of the aircard within defendant's apartment. The FBI personnel did not track defendant's or the aircard's movements or precise location within his apartment. Instead, the personnel used the cell site information to determine a general proximity where the aircard might be found, and then the investigation team supplemented this information with traditional investigative techniques noted above to determine the particular apartment that defendant was using.

Other courts have reached similar conclusions based on the imprecise nature of cell site information. *See, e.g.*, United States v. Suarez-Blanca, 2008 WL 4200156 at *10 (N.D. Ga. Mar.

26, 2008) (finding that "there is no Fourth Amendment search in tracking the location of the cell phone towers used in making phone calls because such towers would not reveal the location of an individual in private quarters"); In Matter of Application of U.S. for an Order, 411 F. Supp. 2d 678, 682 (W.D. La. Jan. 26, 2006) ("Here, however, the cell phone user will not be 'tracked' while in his private residence. The cell site information sought by the Government in this application (and authorized by the court herein) does not permit detailed tracking of a cell phone user within any residence or building. Indeed, the Government will not be able to pinpoint which room, house or building (if any) the user is in."); In re Application of the U.S. for an Order, 405 F. Supp.2d 435, 449 (S.D.N.Y. 2005) ("The collection of information relating to the location of cell towers does not pinpoint a user's location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower. These towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more apart even in urban areas."). *But see* United States v. Finley, 477 F.3d 250, 258-59 (5th Cir.2007) (defendant had expectation of privacy to challenge the actual physical search of a cell phone after arrest where even though employer issued cell phone to defendant, defendant maintained a property interest in the phone, had a right to exclude others from using it, was authorized to use it for both business and personal calls, exhibited a subjective expectation of privacy in it, and took normal precautions to maintain his privacy in the phone).

With respect to the identification of cell phone transmissions, in contract to the physical search of an actual cell phone, numerous courts have held that there is no reasonable expectation of privacy in broadcasts an individual makes over the public airwaves which are knowingly exposed to everyone in the area by virtue of transmission, and can be overheard by anyone having a radio receiver tuned into the same channel. *See* Johnson v. Hawe, 388 F.3d 676, 684 (9th Cir. 2004); City of Sequim, Washington v. Johnson, 544 U.S. 1048 (2005); United States v. Basey, 816 F.2d 980, 993 n. 21 (5th Cir. 1987). *See also* United States v. Hoffa, 436 F.2d 1243, 1247 (7th Cir. 1970) (no reasonable expectation of privacy in calls made from mobile phones where calls exposed to everyone in the area who possessed an appropriate receiver);

United States v. Ahrndt, 2010 WL 373994 at *4-5 (D.Or. 2010) (reduced reasonable expectation of privacy in unsecured wireless networks since data transmitted over radio waves, and therefore easy to intercept wireless transmissions); and Edwards v. Bardwell, 632 F.Supp. 584, 589 (M.D.La. 1986) (no reasonable expectation of privacy in a communication broadcast by radio in all directions that could be overheard by countless people who have appropriate receiving devices).

In this case, the FBI personnel tracked the defendant's aircard transmissions made over public airwaves, using equipment tuned to the same frequency as the aircard. Therefore, defendant could not have had a reasonable expectation of privacy over the radio emanations from his aircard.

Any reliance on Kyllo v. United States, 533 U.S. 27 (2001), in this case would be misplaced. The thermal imaging device used in Kyllo provided information about the inside of a particular residence (and, in fact, clearly differentiated it from neighboring residences), and the parties argued about the quality of the information obtained and whether the technology could provide "intimate details" about the inside of the residence. *See* 533 U.S. at 37. The Court, however, refused to "develop a jurisprudence specifying which home activities are 'intimate' and which are not," and reaffirmed that "the Fourth Amendment draws 'a firm line at the entrance to the house.'" 533 U.S. at 39-40. The Court further explained that "[t]he Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained." *Id.* at 37. In the present case, however, no information at all was collected about the interior of any particular apartment, including defendant's, and no electronically enhanced "search" was conducted of defendant's individual apartment. The subject equipment only led its operators to the general public area where the aircard was in operation. [2/]

[2/] Of course, the obvious difference between the thermal imaging at issue in Kyllo and the cell-site location techniques at issue in the present case is judicial authorization. In Kyllo, (continued...)

b. Cell site records.

Moreover, defendant does not have a reasonable expectation of privacy concerning the cell-site records maintained by Verizon Wireless. These cell-site records are the business records maintained by a third-party carrier as part of the ordinary course of business, and courts have repeatedly held that people do not have a privacy interest in business records voluntarily turned over to third parties. In Smith v. Maryland, the Supreme Court held that the installation of a pen register on the defendant's phone was not a Fourth Amendment "search," as telephone users realize that they convey phone numbers to the telephone company, which has the capability of recording the numbers they dial for the purpose of compiling their monthly bill. 442 U.S. 735, 742 (1979). The Ninth Circuit later relied on Smith to reach their holding in United States v. Forrester that the installation of a pen register analogue, or "mirror port," on an Internet account was not a search in violation of the Fourth Amendment. 512 F.3d 500, 510 (9th Cir. 2007). The Court stated, "e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." *Id.*; *see also* United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("It is well-settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities,

---

[2/] (...continued)
the United States claimed that its thermal imaging did not constitute a search, and therefore it needed no judicial authorization. Here, however, the United States obtained judicial authorization, including a warrant founded on probable cause, to conduct its cell-site tracking mission. The lack of judicial authorization Kyllo is not the only obvious difference. The other is that in Kyllo, use of the infrared equipment provided a visual depiction concerning some of the activities inside the house that no one could have known without entering the house. The thermal heat waves were passively released by the defendant in Kyllo, and law enforcement took advantage of that passive transmission to gain knowledge of the interior of the home. Here, defendant actively and intentionally broadcast radio waves from inside of his apartment to the outside, fulling intending to do so. The interception of these radio waves did not reveal any information concerning the inside of defendant's individual apartment, and in fact, the FBI personnel were unable to identify even which specific apartment was in use by the defendant.

and if that occurs the Fourth Amendment does not prohibit governmental use of that information.").

In the present case, defendant voluntarily turned over cell site information to Verizon Wireless while using the aircard. He should have known that such information was gathered through the normal course of business, and that he therefore had no reasonable expectation of privacy in the related cell-site records. *Cf.* United States v. Suarez-Blanca, 2008 WL 4200156 at *8 (N.D. Ga. Apr. 21, 2008) ("[T]he Court finds that the historical cell site information is akin to other business records maintained in the course of business. Since individuals do not have an expectation of privacy in these other business records, there can be no Fourth Amendment violation based on law enforcement's decision to seek records from cell phone providers about the cell towers associated with past cell phone calls.").

Thus, defendant had no reasonable expectation of privacy in the general proximity of the aircard. As a result, there can be no Fourth Amendment violation, and the privileged information that defendant seeks cannot form the basis for a motion to suppress evidence.

c. Standing.

Finally, even if determining the general proximity of the aircard somehow implicates the Fourth Amendment, defendant lacks standing because it was registered to a fictitious identity. In Rakas v. Illinois, the Supreme Court held that "[a] person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed . . . it is proper to permit only defendants whose Fourth Amendment rights have been violated to benefit from the [exclusionary] rule's protections." 439 U.S. 128, 134 (1978). After Rakas, the relevant inquiry is no longer whether the defendant has "standing" to claim the protections of the exclusionary rule, but rather "whether the defendant's rights were violated by the allegedly illegal search or seizure." United States v. Salvucci, 448 U.S. 83, 88 n.4 (1980). However, "the term 'standing' has been used by courts since Rakas as shorthand for the existence of a privacy or possessory interest sufficient to assert a Fourth Amendment claim."

United States v. Daniel, 982 F.2d 146, 149 n.2 (5th Cir. 1993).

Some courts have held that defendants lack standing to challenge searches of items registered or addressed to a fictitious name or alias, reasoning that defendants abandoned their objective expectation of privacy by using a false identity. *See* United States v. Lewis, 738 F.2d 916, 920 n.2 (8th Cir. 1984) ("A mailbox bearing a false name with a false address and used only to receive fraudulently obtained mailings does not merit an expectation of privacy that society is prepared to recognize as reasonable."); United States v. DiMaggio, 744 F. Supp. 43, 46 (N.D.N.Y. 1990) ("With respect to the unidentified sender, it is as if the package had been abandoned since by withholding from society that he is the source, he has effectively repudiated any connection or interest in the item vis-a-vis society, and no longer has the means to exclude others from intruding upon the contents of the package.") (citation omitted); *cf*. United States v. Lozano, 623 F.3d 1055, 1064 (9th Cir. 2010) (O'Scannlain, concurring) (arguing that "a defendant has no legitimate expectation of privacy in mail addressed to his public alias when that alias was used solely in a criminal scheme," and citing cases from Fifth, Seventh, and Eighth Circuits). *But see* United States v. Villarreal, 963 F.2d 770, 773 (5th Cir. 1992) ("Although the consignee of the drums was technically a fictitious person named Roland Martin, this court has made clear that individuals may assert a reasonable expectation of privacy in packages addressed to them under fictitious names").

Courts have also applied this limitation in cases in which a tracked cell phone is registered or used by a third party, or is registered to an alias. *See* United States v. Suarez-Blanca, 2008 WL 4200156 at *7 (N.D. Ga. Mar. 19, 2009) ("the subscriber information relating to another person or a fictitious person undercuts any claim that [defendant] has a subjective privacy interest in the cell phone and thus the historical cell site information from the phone"); United States v. Bermudez, 2006 WL 3197181 at *13 (S.D. Ind. June 30, 2006) (defendant who did not possess or use co-defendant's phone "cannot suppress the evidence gained from the government's tracking of the [co-defendant's] phone"); United States v. Skinner, 2007 WL 1556596 at *14-15 (E.D. Tenn. May 24, 2007) (defendant lacked standing to challenge

monitoring of a cell phone purchased and provided by a third party for use in drug trafficking operation).

Here, the aircard was obtained by defendant through the use of a false identity in the name "Travis Rupard." In light of defendant's extensive and ongoing efforts to conceal his true identity, it is extremely unlikely that "Travis Rupard" was an alter ego used primarily by defendant for anything but unlawful purposes, he therefore would continue to lack standing to challenge the discovery of the aircard's location. Defendant would not be asserting a privacy interest in the same way that he might have an interest in his home or his computer – or some other closed container – in that it stores private information hidden from public view. [3/] Instead, he would merely be asserting a privacy interest in hiding the location of an item procured by fraud. There is simply no good reason why society should recognize this as a legitimate privacy interest.

d. Kyllo v. United States, 533 U.S. 27 (2001)

In Kyllo v. United States, 533 U.S. 27 (2001), the Supreme Court held that use of sense-enhancing technology to gather any information regarding the interior of home that could not otherwise have been obtained without physical intrusion into constitutionally protected area constitutes a "search." In this case, no information was collected about the interior of any particular apartment and no electronically enhanced "search" was conducted of defendant's apartment. The subject equipment only led its operators to the general area where the aircard was in operation.

In Kyllo, the Supreme Court also held that "a Fourth Amendment search does not occur – even when the explicitly protected location of a house is concerned-unless "the individual

---

[3/] Defendant still had a reasonable expectation of privacy in the apartment itself, even though he rented it under an assumed identity, because the apartment complex had not yet discovered the fraud and attempted to evict him. *See* United States v. Cunag, 386 F.3d 888 (9th Cir. 2004) ("[I]n the Ninth Circuit, the rule is that even if the occupant of a hotel room has procured that room by fraud, the occupant's protected Fourth Amendment expectation of privacy is not finally extinguished until the hotel justifiably takes 'affirmative steps to repossess the room.'").

manifested a subjective expectation of privacy in the object of the challenged search," and "society [is] willing to recognize that expectation as reasonable." Kyllo, 533 U.S. at 32. In this case, defendant did not manifest a subjective expectation of privacy in the radio signals emanating from the aircard. Instead, at the time the aircard was in operation, as discussed above, defendant fully intended that the device's signals leave his residence and travel to the service provider's cell towers in order for defendant to receive service. Since defendant voluntarily transmitted the signal to all with a radio receiver in the area and disclosed the cell information to a third party, he had no reasonable expectation of privacy over the aircard's signal and cell tower information. *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("[i]t is well-settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information . . .")

2. Defendant does not need the privileged information because the investigation team obtained and executed the warrant in good faith.

Even if defendant could articulate a Fourth Amendment violation, suppression would not be an appropriate remedy because the FBI personnel and investigation team conducted the tracking operation and follow-up investigation in good faith. The Supreme Court held in United States v. Leon that the fruits of a search must not be suppressed if the police acted in good faith in relying on and executing a warrant later found to be insufficient. 468 U.S. 897 (1984). The exclusionary rule's primary purpose is to deter future unlawful police conduct, and the good faith reliance exception recognizes that if an officer is acting reasonably, excluding the evidence does not positively affect his future conduct. *See* United States v. Calandra, 414 U.S. 338, 347 (1974) (explaining that the primary purpose of the exclusionary rule is deterrence); Leon, 468 U.S. at 920 (stating that, if "the officer is acting as a reasonable officer would and should act in similar circumstances[,] [e]xcluding the evidence can in no way affect his future conduct unless

it is to make him less willing to do his duty").

Here, the FBI personnel located the general location of the aircard in reliance on, among other authorities, the tracking device warrant issued by Judge Seeborg on July 11, 2008. That order authorized a tracking device warrant under Federal Rule of Criminal Procedure 41(b), finding probable cause to believe that the monitoring of the aircard would lead to evidence and the identification of the perpetrators.

The good faith exception applies even if the warrant lacked probable cause, as long as the officers relied on the warrant in an objectively reasonable manner. *See* United States v. Alvarez, 358 F.3d 1194, 1204 n.3 (9th Cir. 2004); United States v. Clark, 31 F.3d 831, 835 (9th Cir. 1994). In addition, the Ninth Circuit has specified four circumstances in which the good faith exception does not apply because reliance on a warrant is per se unreasonable:

> (i) where an affiant misleads the issuing magistrate or judge by making a false statement or recklessly disregarding the truth in making a statement; (ii) where the magistrate or judge wholly abandons her judicial role in approving the warrant, acting only as a "rubber stamp" to the warrant application rather than as a neutral and detached official; (iii) where the warrant is facially deficient in detail as to the place to be searched or the things to be found that the officers could not reasonably presume it to be valid; or (iv) where the affidavit upon which the warrant is based is so lacking in indicia of probable cause that no reasonable officer could rely upon it in good faith.

United States v. Crews, 502 F.3d 1130, 1136 (9th Cir. 2007). None of these four circumstances apply in the present case.

Thus, defendant's interest in the privileged information cannot result in suppression even if the tracking operation implicates the Fourth Amendment. Defendant may disagree with the United States' legal theory for obtaining the information or the magistrate judge's decision to issue the order, but the fact remains that the agents relied on and executed the warrant in good faith.

3. Defendant does not need the privileged information because, in the absence of a Constitutional violation, suppression is not a remedy.

Defendant argues that he needs access to the requested discovery in order to fully develop his motion to suppress. According to 18 U.S.C. § 2708, however, "The remedies and sanctions

described in [the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712] are the only judicial remedies and sanctions for nonconstitutional violations of [the SCA]." Remedies include criminal fines and imprisonment under 18 U.S.C. § 2701(b) for unlawful access to stored communications, and civil remedies such as damages and administrative discipline under 18 U.S.C. § 2707 for any knowing or intentional violations of the SCA. Suppression of evidence is not listed. And the Ninth Circuit has acknowledged that suppression is not an appropriate remedy for violations of the SCA. *See* United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998) ("[T]he Stored Communications Act does *not* provide an exclusion remedy. It allows for civil damages . . . and criminal punishment . . . but nothing more.") (citations omitted).

The provisions of the United States Code governing the installation and use of pen registers and trap and trace devices also exclude suppression as an appropriate remedy. Instead, the only penalty specified is that those who "knowingly violate[] subsection (a)" by installing or using a pen register or trap and trace device without obtaining a court order "shall be fined under this title or imprisoned not more than one year, or both." 18 U.S.C. § 3121(d). The Ninth Circuit has held that suppression of evidence gathered in violation of the pen register statute is "plainly inappropriate." Forrester, 512 F.3d at 512-513; *see also* United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) ("[T]he statutory scheme [of the pen register statute] does not mandate exclusion of evidence for violations of the statutory requirements"); United States v. Thompson, 936 F.2d 1249, 1249-1250 (11th Cir. 1991) ("We hold that information obtained from a pen register placed on a telephone can be used as evidence in a criminal trial even if the court order authorizing its installation does not comply with the statutory requirements."). The court in Forrester stated that "suppression is a disfavored remedy, imposed only where its deterrence benefits outweigh its substantial social costs or (outside the constitutional context) where it is clearly contemplated by the relevant statute." 512 F.3d at 512. This limited application of the exclusionary rule is in line with Supreme Court precedent. *See, e.g.*, Hudson v. Michigan, 547 U.S. 586, 591 ("Suppression of evidence . . . has always been our last resort, not our first impulse.").

Thus, defendant has no need for the privileged information because he cannot challenge the application of the SCA in this proceeding. His objections to the United States' legal theories underpinning the tracking operation—for example, his challenge to the "after receipt and storage" requirement, or his speculation that the agents may have exceeded the scope of their authority under the SCA—may form the basis for a civil suit or some other remedy within the SCA, but it cannot lead to suppression of evidence in his criminal case.

III. Conclusion

For the foregoing reasons, information related to the nature and use of the law enforcement sensitive equipment used to generally locate the subject aircard is privileged and should not be released to defendant. Moreover, there is not one scintilla of evidence in this case that the personnel who operated the subject detection equipment, or the members of the investigation team who followed up on their general findings, ever conducted any type of search of defendant's apartment prior to the execution of fully authorized search warrant. Accordingly, defendant's request for the subject information should be denied. Should the Court desire additional information regarding the sensitive nature of the subject equipment *ex parte* and *in camera*, the government is willing to prepare for, and appear at, such a hearing.

Respectfully submitted this 11th day of March, 2011.

DENNIS K. BURKE
United States Attorney
District of Arizona

S/Frederick A. Battista

FREDERICK A. BATTISTA
PETER S. SEXTON
JAMES R. KNAPP
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that on March 11, 2011, I caused the attached document to be electronically transmitted to the Clerk's Office using the ECF system for filing and transmittal of a Notice of Electronic Filing to the following ECF registrants:

Philip Seplow
Shadow Counsel for Defendant Daniel David Rigmaiden

Taylor Fox
Counsel for Defendant Ransom Carter

A copy of the attached document was also mailed to:

Daniel David Rigmaiden
Agency No. 10966111
CCA-CADC
PO Box 6300
Florence, AZ 85132

S/Frederick A. Battista

FREDERICK A. BATTISTA
Assistant U.S. Attorney